Expert Sniffer® Technology

Network General's Approach to Solving Network Problems

Network General®

We solve network problems.™

Introduction

Expert Sniffer® Technology will revolutionize the process of network design, implementation and management by placing the intelligence of a network expert into the hands of every network manager. This will be a boon to both experienced and inexperienced network managers, and will change the way professionals charged with the responsibility of managing a valuable corporate resource are expected to function.

The benefits provided by this new technology are:

- Provides answers, not just data, to solve complex network problems in the shortest time possible, thus preventing network downtime and performance problems
- Avoids network downtime and performance slowdowns by finding symptoms before they result in problems
- Puts years of Network General's troubleshooting technology into users' hands to dramatically increase network manager's productivity

These benefits reduce the real costs of running a network — the ongoing operating expenses.

This paper provides:

1. An overview of how Expert Sniffer Technology delivers these benefits

2. Examples of the types of problems Expert Sniffer Technology solves

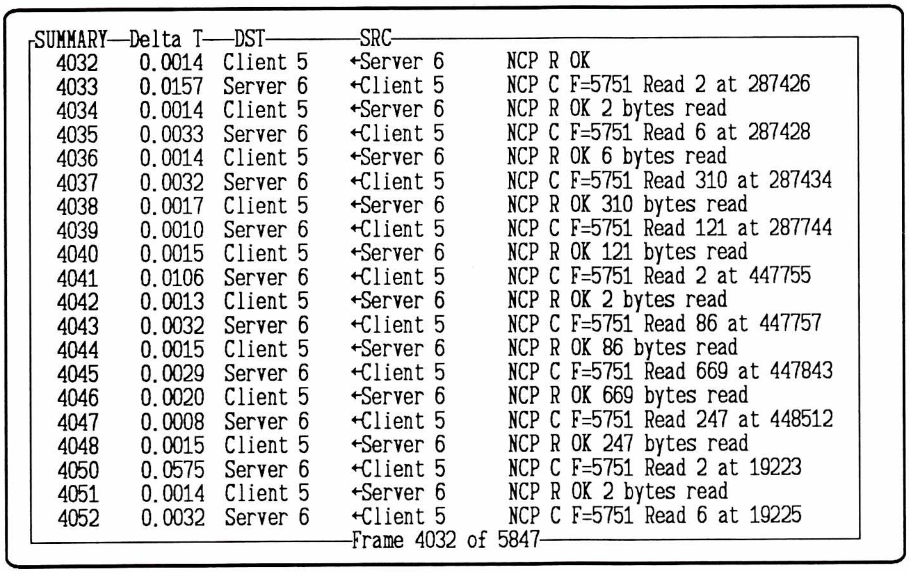
3. A detailed technical background on the Technology

4. Future directions for Expert Sniffer Technology

Overview of the Technology

The main goal of the Expert Sniffer Technology is to put years of network troubleshooting experience into users' hands. Rather than simply being a tool that facilitates problem solving (but has no intelligence to draw on) this new technology allows customers to take advantage of the collective expertise amassed through years of Network General's focused troubleshooting effort.

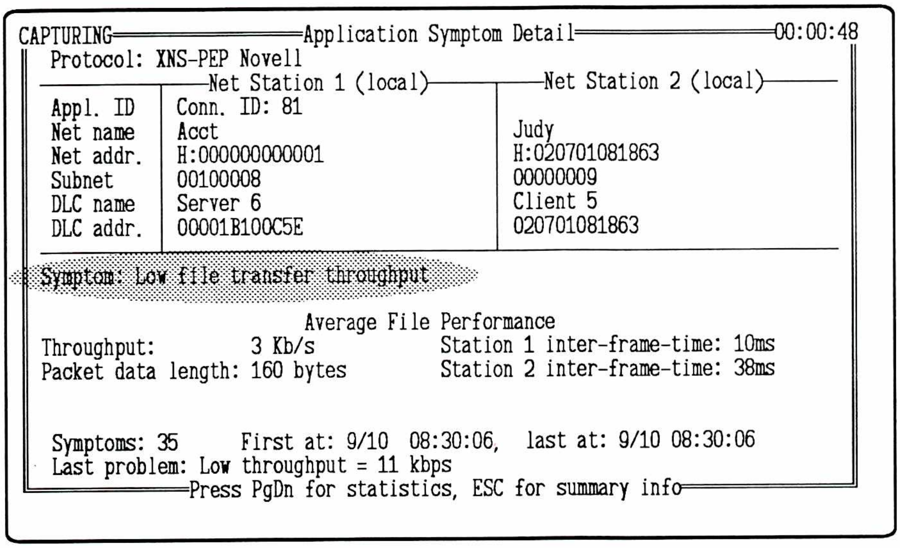
Expert Sniffer Technology solves fault and performance problems at all seven layers of the network. To understand how this approach differs from current protocol analyzers, think of the analyzer as an X-ray machine. An X-ray enables one to see the bone structure of the patient, but a specialized technician is still required to interpret the findings and a doctor to make the final diagnosis. Expert Sniffer Technology combines the roles of the X-ray machine, technician, and doctor into one, creating a system that identifies, interprets and diagnoses network problems or performance irregularities. This frees the network manager to focus on corrective action.



```
SUMMARY—Delta T——DST—————SRC——————————————————————————————————
  4032  0.0014  Client 5  ←Server 6    NCP R OK
  4033  0.0157  Server 6  ←Client 5    NCP C F=5751 Read 2 at 287426
  4034  0.0014  Client 5  ←Server 6    NCP R OK 2 bytes read
  4035  0.0033  Server 6  ←Client 5    NCP C F=5751 Read 6 at 287428
  4036  0.0014  Client 5  ←Server 6    NCP R OK 6 bytes read
  4037  0.0032  Server 6  ←Client 5    NCP C F=5751 Read 310 at 287434
  4038  0.0017  Client 5  ←Server 6    NCP R OK 310 bytes read
  4039  0.0010  Server 6  ←Client 5    NCP C F=5751 Read 121 at 287744
  4040  0.0015  Client 5  ←Server 6    NCP R OK 121 bytes read
  4041  0.0106  Server 6  ←Client 5    NCP C F=5751 Read 2 at 447755
  4042  0.0013  Client 5  ←Server 6    NCP R OK 2 bytes read
  4043  0.0032  Server 6  ←Client 5    NCP C F=5751 Read 86 at 447757
  4044  0.0015  Client 5  ←Server 6    NCP R OK 86 bytes read
  4045  0.0029  Server 6  ←Client 5    NCP C F=5751 Read 669 at 447843
  4046  0.0020  Client 5  ←Server 6    NCP R OK 669 bytes read
  4047  0.0008  Server 6  ←Client 5    NCP C F=5751 Read 247 at 448512
  4048  0.0015  Client 5  ←Server 6    NCP R OK 247 bytes read
  4050  0.0575  Server 6  ←Client 5    NCP C F=5751 Read 2 at 19223
  4051  0.0014  Client 5  ←Server 6    NCP R OK 2 bytes read
  4052  0.0032  Server 6  ←Client 5    NCP C F=5751 Read 6 at 19225
——————————————————————————Frame 4032 of 5847——————————————————————
```

Fig. 1 Current Sniffer Technology

Look at the Sniffer Network Analyzer screen to the left. A trained technician can see that a Novell NetWare client is reading a file from the server. A knowledgeable network manager might observe that transaction throughput is low by examining the read byte sizes and the time between packets.



```
CAPTURING════════════════Application Symptom Detail══════════════00:00:48
  Protocol: XNS-PEP Novell
  ──────────────Net Station 1 (local)──────────Net Station 2 (local)──────
  Appl. ID   │ Conn. ID: 81             │
  Net name   │ Acct                     │ Judy
  Net addr.  │ H:000000000001           │ H:020701081863
  Subnet     │ 00100008                 │ 00000009
  DLC name   │ Server 6                 │ Client 5
  DLC addr.  │ 00001B100C5E             │ 020701081863
  ────────────────────────────────────────────────────────────────────────
  Symptom: Low file transfer throughput

                       Average File Performance
 Throughput:          3 Kb/s          Station 1 inter-frame-time: 10ms
 Packet data length: 160 bytes        Station 2 inter-frame-time: 38ms


  Symptoms: 35      First at: 9/10  08:30:06,   last at: 9/10 08:30:06
  Last problem: Low throughput = 11 kbps
═══════════Press PgDn for statistics, ESC for summary info═══════════════
```

Fig. 2 Expert Sniffer Technology

The Expert Sniffer Technology has determined there is a file transfer in progress, and makes a judgement that the file throughput is too low. Below the conclusion are some statistics that backup the system's determination of low throughput. In addition, with a single keystroke the network manager can examine the actual packets the system analyzed to detect the problem. Using this information, the network manager can determine what parameters to correct on the file server and workstation.

Network Problems and Their Solutions

Expert Sniffer Technology's logical format and intuitive system provide network managers with three types of diagnostic information:

- **Symptoms**
- **Diagnoses**
- **Explanations and Conclusions**

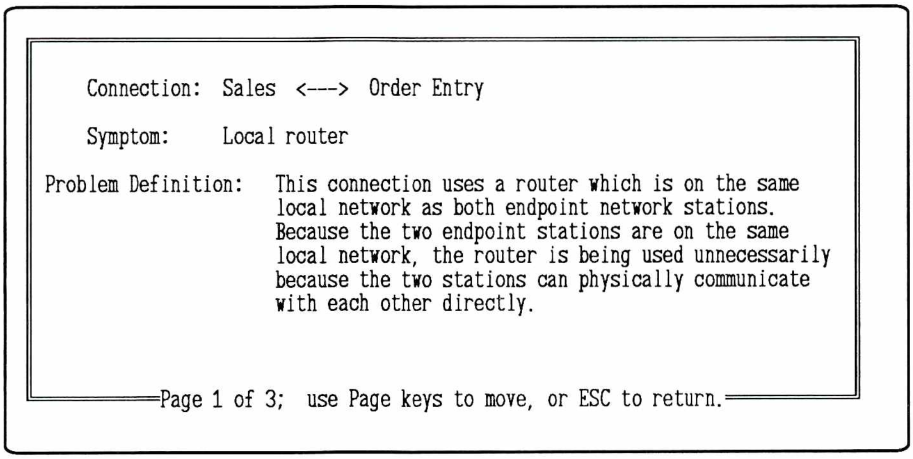
To provide Explanations and Conclusions, the technology first examines the network for **symptoms.** By itself, a **symptom** is not necessarily a fault, but could indicate a network problem. For example, a single file retransmission is not necessarily a problem. The network continues to function, and users continue to perform their work. However, when file retransmissions happen 50 times in a row on the same file, or retransmits repeatedly over a few seconds, network behavior is not normal. In this case, the system will propose a **diagnosis.** A **diagnosis** is something that, in the judgement of the system, the network manager ought to take action on.

The system then provides an explanation of its conclusions on both the diagnosis and the symptoms that led to the diagnosis and recommends corrective action. The system can perform this function for over 100 common network problems. Examples of such problems are:

- Slow File Transfers
- Inefficient Network Routing
- Transport Retransmissions
- Broadcast Storms
- Misconfigured Retransmission Timers
- Repetitive Loops on Application Requests

These types of problems span multiple topologies (Ethernet, Token Ring, etc.) and are often found in multiple protocols (TCP/IP, DECnet®, NetWare®, NFS®, etc.)

In the three screens below, the system has identified a local router problem. Local routers are potential problems because they double the amount of network traffic on a segment and waste valuable router bandwidth. Figure 3 defines at the local router problem. The next screen draws a context sensitive network diagram showing how the local router is used for communication between two stations on the same local network. The last screen offers suggestions for corrective action. In order to perform this diagnosis, the system had to learn the network names, station types, and routing patterns, and then apply that knowledge to identify the problem in real time.



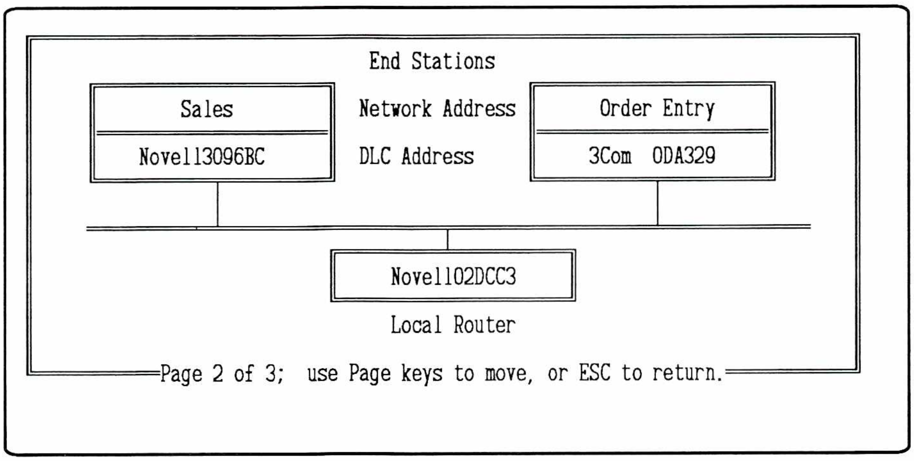
```
    Connection:  Sales  <---> Order Entry

    Symptom:     Local router

Problem Definition:   This connection uses a router which is on the same
                      local network as both endpoint network stations.
                      Because the two endpoint stations are on the same
                      local network, the router is being used unnecessarily
                      because the two stations can physically communicate
                      with each other directly.

          Page 1 of 3;  use Page keys to move, or ESC to return.
```

Fig. 3 Local Router Definition

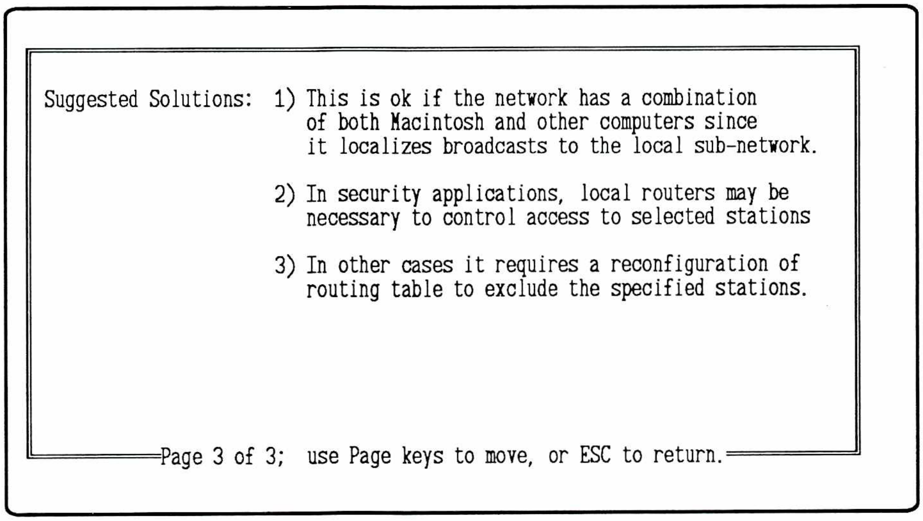


```
                            End Stations
        Sales             Network Address        Order Entry
     Novell3096BC         DLC Address           3Com  0DA329

                           Novell02DCC3
                           Local Router

          Page 2 of 3;  use Page keys to move, or ESC to return.
```

Fig. 4 Local Router Explanation



```
Suggested Solutions:  1) This is ok if the network has a combination
                         of both Macintosh and other computers since
                         it localizes broadcasts to the local sub-network.

                      2) In security applications, local routers may be
                         necessary to control access to selected stations

                      3) In other cases it requires a reconfiguration of
                         routing table to exclude the specified stations.

          Page 3 of 3;  use Page keys to move, or ESC to return.
```

Fig. 5 Local Router Solution

One Solution Opens the Door

In order to allow network managers to effectively solve network problems, Network General's biggest challenge was to analyze real time data moving at high data rates at all seven network layers. Several years of intense research and much trial and error resolved that challenge. Having met this challenge, Network General focused on other features essential to real time, proactive, intelligent analysis systems:

- The system had to automatically identify problems in real time so network managers could proactively find complex network faults before they cause downtime;
- Since network elements such as topologies, traffic flows, appications, etc. change so quickly, the system had to have the capacity to learn about individual network characteristics in order to provide network-specific solutions;
- With such vast amounts of data flowing across networks, the system had to "forget" or discard unwanted information no longer required for problem analysis;
- Because network managers usually do not know what are the symptoms that caused the problems in advance, the system has to have the ability to tell the network manager what the problem was without the need to input a hypothesis;

Real Time Automatic Problem Identification

An Ethernet network utilized at 10% of capacity generates 10 billion bytes of data in 24 hours. No system can store this amount of information to analyze in off-peak times. Therefore, an expert system must process each packet as it flows across the network, and then move on to the next packet.

Expert Sniffer Technology does this by extracting useful information from each packet and then grouping the information into a relatively small number of "logical objects" that characterize network communication. An "object" can be an application connection between station A and station B or it can be a network level address. By continually updating all objects about which a packet carries information, the Expert Sniffer Technology can quickly move onto the next packet. This technique can reduce 20,000 packets down to 200 "objects" and in so doing allow analysis to occur in real time.

Learning about the Network

Every network is unique. Networks also change constantly and rapidly. Even the most meticulous network manager cannot maintain detailed records about network configuration, traffic flows, names, station types, protocols, etc. Therefore, it was essential to build into the Expert Sniffer Technology the heuristic ability to automatically learn the specifics of a particular network to which it is attached. Based on this knowledge, the system can provide the user with network-specific analyses, explanations, and conclusions. For example, in the previous local router example, the system was able to learn station names, routing paths, and configuration information and apply that information to formulate a detailed explanation of the problem.

"Forgetting" Outdated Information

Over time, the amount of network management information quickly grows beyond the ability of the user to view and understand it. A key attribute of the Expert Sniffer Technology is the ability to discard outdated information. If a normal conversation happened between two stations yesterday, the system does not need to keep a record of that conversation. Since the user will never examine it, the system needs to determine which information is unnecessary and then "forget" it, thereby keeping the network management database to a manageable size.

Getting Answers to Problems without Entering Hypotheses

Network managers cannot be expected to know what is happening on the network at all times. Typically expert systems require the user to enter a hypothesis, such as "I can't connect to Station Fred. Is the router down?" To be truly proactive, network managers require systems that can tell them a station is down and why *before* the user calls. Expert Sniffer Technology is designed to continuously examine the network for problems in real time and alert the manager to them.

Revolutionary Technology Required for Networks

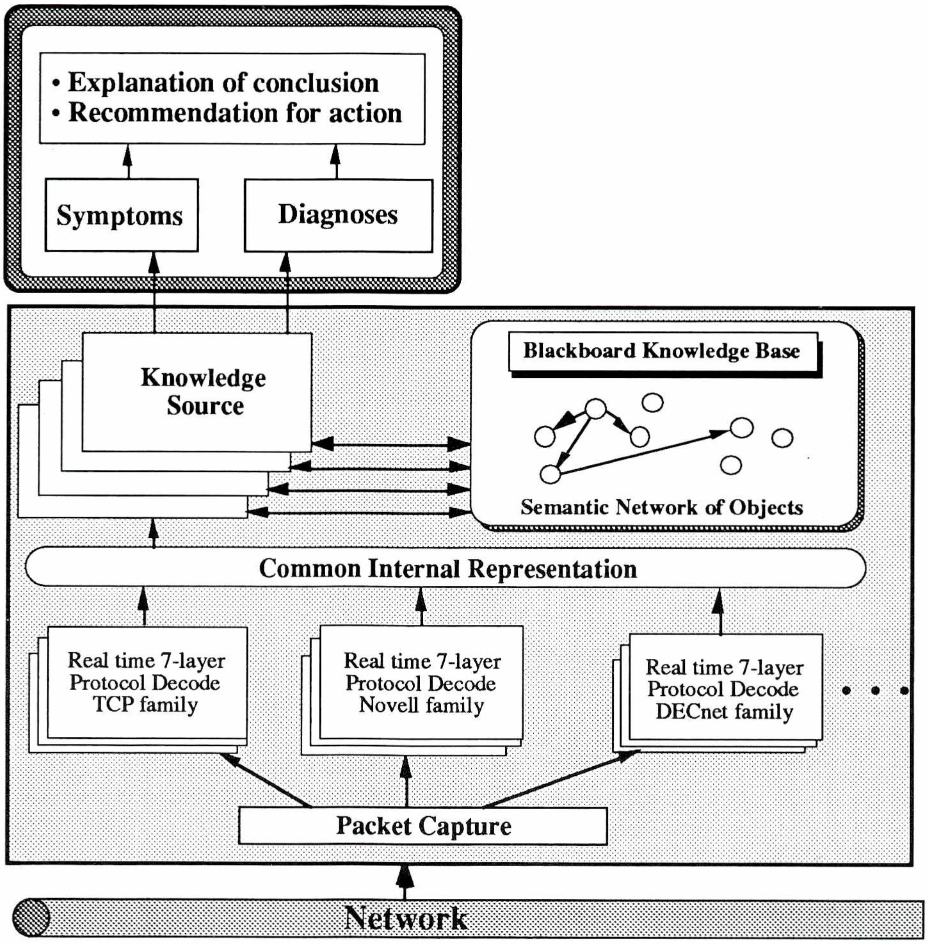

• Explanation of conclusion
• Recommendation for action
Symptoms
Diagnoses
Knowledge Source
Blackboard Knowledge Base
Semantic Network of Objects
Common Internal Representation
Real time 7-layer Protocol Decode TCP family
Real time 7-layer Protocol Decode Novell family
Real time 7-layer Protocol Decode DECnet family
• • •
Packet Capture
Network

Fig. 6 Expert Sniffer Technology

To meet the challenges peculiar to real time networks, Network General developed its expert technology starting from the latest theoretical and prototype work done at Stanford University[1], the University of Massachusetts[2], and Nippon Telephone and Telegraph (NTT)[3]. Leveraging off this work, Network General has spent several years evaluating, modifying, and adapting various expert methodologies in unique ways to create its Expert Sniffer Technology. In addition to studying the adaptability of a variety of expert technologies to real time networks, over the last six years Network General has been continuously developing the most complete set of protocol decodes which now number over 120. These decodes, which underlay the expert features of the system, are filled with very detailed protocol information that has been expanded to create decode modules that function in real time.

Starting at the bottom of the diagram above, Expert Sniffer Technology captures packets off the network and feeds them to a set of real time protocol decode modules. As the decode modules notice various conditions (i.e., a wrong reply sequence, the start of a file transfer, or a new network layer address), they put them in a "common internal representation" for a Knowledge Source to examine. A Knowledge Source detects a class of problems across many network types by looking for generalized types of problems across protocols. This provides very powerful problem detection in a multi-vendor, multi-protocol environment. It also makes Expert Sniffer Technology easily extensible to additional network problems. For example, to detect a duplicate IP address (TCP/IP network layer address), the Knowledge Source looks for duplicate network layer addresses. It does not matter if the protocol is Novell NetWare, DECnet, or TCP/IP.

[1] Hitson, Bruce L. "Knowledge-Based Monitoring and Contol of Distributued Systems," Technical Report Number CSL-TR-90-414, Stanford University, February, 1990.
[2] Lesser, V. et al. "A High-Level Simulation Testbed for Cooperative Distributed Problem-Solving," Computer and Information Science, University of Massachsusetts at Amherest, March, 1981.
[3] Sugawara, Toshiharu. "A Cooperative LAN Diagnostic and Observation Expert System, IEEE Proceedings of the IEEE Phoenix International Conference on Computers and Communication, 1990 pp. 667-674.

The Knowledge Source then posts selected information to the Blackboard Knowledge Base. Blackboard Systems[4] are an expert system problem solving technique developed in the late '70's to cope with ill-defined, complex applications in speech recognition which required dealing with changing conditions in real time. Think of the Blackboard as a place where the various Knowledge Sources place their discoveries. Each separate knowledge source is constantly posting information to the Blackboard and examining the Blackboard for symptom and diagnosis conditions.

Expert Sniffer Technology stores network information in a Semantic Network of Objects on the Blackboard. Recall that an object can be a connection between Station A and B, a description of a router, or a set of application transactions (i.e., file transfers) between two stations. Objects are the *key* to the system storing the most important information necessary to identify problems. Object-oriented methods provide for generalized handling of information where appropriate, yet are adaptable to topology or protocol-specific issues as required.

In combination, these expert technologies create a very powerful Expert Sniffer architecture that can deal with the realities of today's complex, changing networks to solve a wide variety of perplexing network problems in high performance environments.

Processing Requirements

Available for Low to Mid-level CPU Power

One of the goals for Expert Sniffer Technology is to run on widely available, inexpensive hardware platforms. To run reliably, the system requires dedicated processing power. Expert Sniffer Technology operates on Intel 386SX or higher class processors with at least four megabytes of memory. Slower processors (i.e. Intel 8088, 80186 or equivalent from Motorola) with 1-2 megabytes of memory do not have the storage capacity to retain important network diagnostic information nor the processing power to perform powerful problem analyses. However, to keep costs as low as possible, Network General has developed this technology without requiring more expensive RISC-based and multi-processing technologies.

One of the main advantages of these processing requirements is that Network General has protected its customers' investments in current Sniffer Network Analyzers and Distributed Sniffer System Servers. These products will support Expert Sniffer Technology by means of a simple software upgrade.

Future Directions

Expert Sniffer Technology is a base for the development of increasingly intelligent and powerful network analysis tools and systems. Network General's current implementation is based on the stand-alone, portable Sniffer Network Analyzer. Having developed the foundation, Expert Sniffer Technology will expand in these important directions:

Distributed Expert System - A version of our Distributed Sniffer System (DSS) based on Expert Sniffer Technology will allow users to view expert-level information on an enterprise-wide basis from one or more locations;

Enhanced Problem Analysis - Currently, Expert Sniffer Technology pinpoints over 100 common network problems. Network General is employing "knowledge engineering" to dramatically expand the number of problems analyzed;

Extended Protocol and Topology Support - Network General will continue to expand the number of protocols and topologies addressed by the Expert Sniffer Technology. We are expanding our program of collecting problems from Sniffer customers and adding them to future product releases. This strategy began in 1986 when the original Sniffer Network Analyzer platform was introduced with analysis for seven protocols and has expanded over the years to an industry-leading 120.

With our commitment to enhance, extend, and build on the existing product base, customers will continue to benefit from their relationship with Network General instead of obsoleting their investment in network analysis products and training. The major benefit to customers is they will be purchasing Network General's cumulative knowledge base for solving network problems. This is an even more sophisticated and beneficial technology than existing protocol analysis capabilities. In addition, Expert Sniffer Technology will run on all Sniffer Analyzers and DSS products being sold to protect our customer's investment.

[4] Corkill, Daniel. "Blackboard Systems," AI Expert, September, 1991, pp. 41-47.

Expert Sniffer Technology Intergration

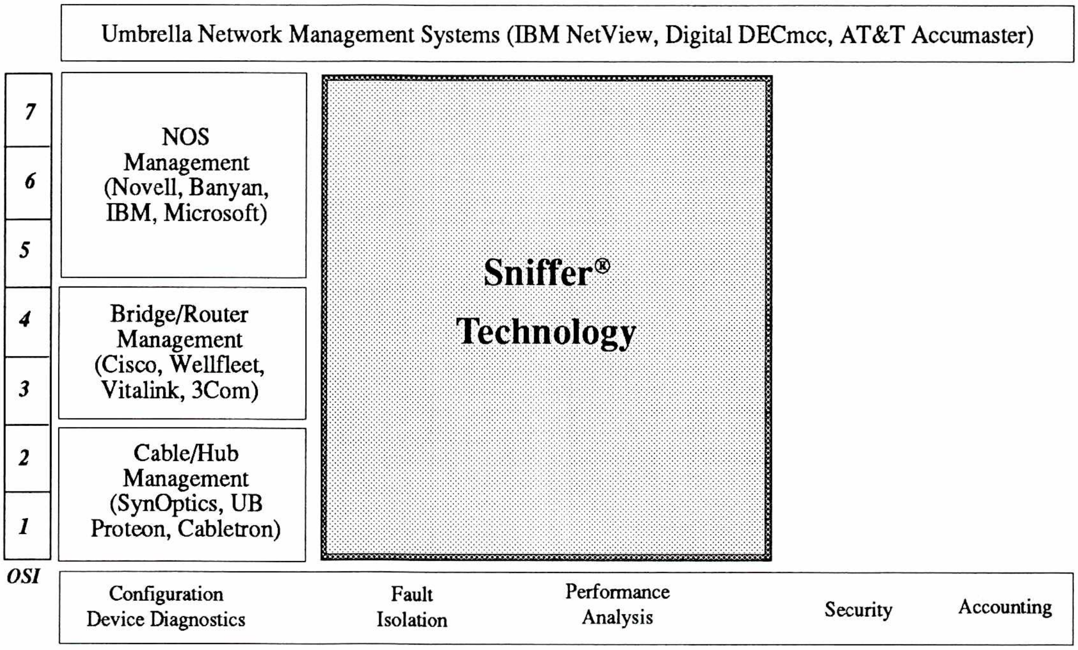

Umbrella Network Management Systems (IBM NetView, Digital DECmcc, AT&T Accumaster)
7
6
5
4
3
2
1
OSI
NOS Management (Novell, Banyan, IBM, Microsoft)
Bridge/Router Management (Cisco, Wellfleet, Vitalink, 3Com)
Cable/Hub Management (SynOptics, UB Proteon, Cabletron)
Sniffer® Technology
Configuration Device Diagnostics
Fault Isolation
Performance Analysis
Security
Accounting

Fig. 7 Sniffer Technology in Network Management Solutions

There are two areas of network management that Network General will integrate with via the distributed version of our Expert Sniffer Technology: standard protocols and umbrella management systems.

Standard network management protocols such as SNMP, CMIP, and NetView's NMVT focus on the control of network elements such as bridges, routers, hubs, front-end processors, etc. Recently, some vendors have started to use these protocols for network monitoring (i.e., OSI level 1 and 2 problems and statistics). Network General will both continue and expand its support of these standards. Sophisticated analysis provided by the Expert Sniffer Technology is not addressed by these standards. Network General is working with standards organizations to develop standards in these areas. It is our intention to support these efforts in our products.

Many network managers will require Expert Sniffer Technology to be integrated with their umbrella management systems (i.e. SunNet Manager, IBM NetView, DECmcc, HP OpenView, etc.). Network General will integrate these systems in two ways:

1) By supporting standard network management protocols as discussed above;

2) By having the Distributed Sniffer System's central console support the same platforms used by many umbrella management systems, thereby allowing simultaneous access to the distributed network analysis servers and the umbrella management system from a single console.

Conclusions

Network General's Expert Sniffer Technology is a base for developing powerful network analysis applications in multi-vendor, multi-protocol environments. It will change the way network managers manage networks by:

- Improving the effectiveness of network professionals by allowing them to easily solve more complex network problems;
- Being truly proactive in identifying and solving problems;
- Dramatically increasing the productivity of network managers by finding complex problems in seconds, instead of hours and days.

For More Information,
Please Contact Your
Network General
Sales Representative.

Further Reading

1) Corkill, Daniel. "Blackboard Systems", AI Expert, September, 1991, pp. 41-47.

2) Sugawara, Toshiharu. A Cooperative LAN Diagnostic and Observation Expert System, IEEE Proceedings of the IEEE Phoenix International Conference on Computers and Communication, 1990, pp. 667-674.

3) Hitson, Bruce L. "Knowledge-Based Monitoring and Control of Distributed Systems," Technical Report No. CSL-TR-90-414, Stanford University, February, 1990.

4) Lesser, V. et al.The HEARSAY-II speech understanding system: integrating knowledge to resolve uncertainty, Computing Surveys, 1980, pp. 213-253.

5) Nii, H. Penny. Blackboard Systems, Report KSL 86-18, Knowledge Systems Laboratory, Stanford University, June 1986.

6) Waterman, Donald A. A Guide to Expert Systems, Addison-Wesley Publishing, Reading, MA, 1986.

7) Lesser, V. et al. "A High-Level Simulation Testbed for Cooperative Distributed Problem-Solving," Computer and Information Science, Univ. of Mass. at Amherst, March, 1981.

8) Winston, Patrick Henry. Artificial Intelligence, Addison-Wesley Publishing, Reading, MA, 1984.

Network General®

We solve network problems.™

Network General Corporation

4200 Bohannon Drive
Menlo Park, CA 94025
TEL: (415) 688-2700
FAX: (415) 321-0855

Network General Europe

Belgicastraat 4
1930 Zaventem (Brussels), Belgium
TEL: 32-2-725-6030
FAX: 32-2-725-6639

PN 24148 12/91